

Authentication methods properties - CustomerID

The authentication methods presented in this section should be created manually at installation-time using the Ubisecure SSO Management.

These configurations are available in the `eidm2.properties` file.

methods.protected

This property defines the accepted authentication methods for user authentication. In other words, this is list of authentication methods used in this installation.

The format of the property value is a comma-separated list of authentication method name property names or directly authentication method names. For example, plain password authentication can be disallowed by removing the name of the password authentication method from this list.

Default is `password.2, saml.ap.custid`

Example:

```
methods.protected = methods.password, methods.sms, methods.otp
```

Ubisecure Password

methods.password

This property defines the password authentication method to be used.

Default is `password.2`

Example:

```
methods.password = password.2
```

password.minLength

This property defines the minimum length of a password.

Default is 8

Example:

```
password.minLength = 8
```

password.pattern.N

The system only accepts passwords that match all the regular expression patterns specified. If you add a new pattern to the list, use the next successive positive integer as its identification number. For example `password.pattern.3`. The password rules you define here need to be at least as strict as any later rules for the password. Later rules may be defined for example in the password method configuration or in the LDAP directory where the passwords will be eventually stored.

Defaults are:

```
password.pattern.1 = [a-zA-Z]
password.pattern.2 = [0-9]
```

Example 1:

```
# Only accept passwords that include alphabetical letters and numbers.
password.pattern.1 = [a-zA-Z]
password.pattern.2 = [0-9]
```

Example 2:

```
# Only accept passwords that contain characters from at least 3 of the
# following 4 rules:
# 1) Upper case letters
# 2) Lower case letters
# 3) Numbers
# 4) Non-alpha numeric
password.pattern.1 = ^(?: (?=.*[a-z\\xE4\\xF6\\xE5]) (?=.*[A-Z\\xC4\\xD6\\xC5]) (?=.*[\\d[^\P{L}\P{Nd}]]) | (?=.*[^\P{L}\P{Nd}]) (?=.*\\d)) | (?=.*[^\P{L}\P{Nd}]) (?=.*[A-Z\\xC4\\xD6\\xC5]) (?=.*\\d) ).*$
password.pattern.2 =
```

passwordrecovery.protection.configuration

This property defines the protection configuration that is used in password recovery. Only the method list is relevant from the protection configuration related to password recovery.

Default is 1

Example:

```
passwordrecovery.protection.configuration = 1
```

Ubisecure OTP Printout

methods.otp

This property defines the name of the Ubisecure OTP Printout authentication method to be used. If it is left empty then no Ubisecure OTP Printout method will be in use.

Default is <not defined>

Example:

```
methods.otp = ubikey.otp.1
```

methods.otp.table

If the user information is stored in Active Directory, Ubisecure Directory must contain an OTP table under the Ubisecure OTP Printout method. This property defines the name (that is, CN) of the OTP table.

Default is otp.table.1

Example:

```
methods.otp.table = otp.table.1
```

Ubisecure SMS

methods.sms

This property defines the Ubisecure SMS authentication method to be used for SMS authentication. If it is left empty then no Ubisecure SMS method will be in use.

Default is <not defined>

Example:

```
methods.sms = ubikey.sms.1
```

methods.sms.gateway

This property defines the URL for the SMS gateway. The URL will be used as is, except for substituting {mobile} and {challenge} for the mobile number and the challenge to be sent by SMS to the mobile number, respectively.

Default is <not defined>

Example:

```
methods.sms.gateway = http://smsgw/sendsms?PhoneNumber={mobile}&text={challenge}&etc=123
```

TUPAS

methods.tupas

This property defines the enabled Tupas authentication methods as a comma-separated list. If it is left empty then no TUPAS methods will be in use.

Default is <not defined>

Example:

```
methods.tupas = tupas.op.1, tupas.nordea.1,\  
tupas.danske.1, tupas.sppop.1, tupas.tapiola.1
```

Ubisecure Windows Authentication Provider

methods.winap

This property defines the name of the Ubisecure Windows Authentication Provider authentication method to be used. This enables the possibility to use Windows SSO with Ubisecure CustomerID. Please consult the document *Ubisecure Windows Authentication Provider* for instructions on how to install Ubisecure Windows AP to Ubisecure SSO. Add methods.winap to the methods.protected property to make it possible to actually use it with Ubisecure CustomerID.

Default is <not defined>

Example:

```
methods.winap = windows.localdomain.1
```

External Methods

methods.external

This property defines the names of external authentication methods (not TUPAS methods) as a comma-separated list. If it is left empty then no external authentication methods will be in use.

Default is <not defined>

Example:

```
methods.external = saml.idp.1, pki.ubilogin.1
```